(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 4 231 256 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
23.08.2023 Patentblatt 2023/34

(21) Anmeldenummer: **22207943.6**

(22) Anmeldetag: **17.11.2022**

(51) Internationale Patentklassifikation (IPC):
G07C 9/00 *(2020.01)*

(52) Gemeinsame Patentklassifikation (CPC):
G07C 9/00309; G07C 9/00896; G07C 2209/04

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC ME MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA
Benannte Validierungsstaaten:
KH MA MD TN

(30) Priorität: **22.02.2022 EP 22157856**

(71) Anmelder: **EUCHNER GmbH + Co. KG**
70771 Leinfelden-Echterdingen (DE)

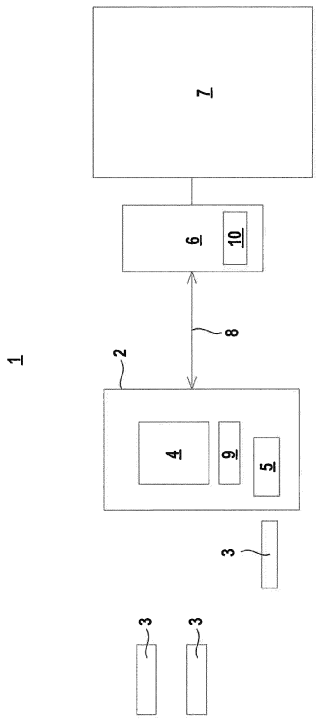
(72) Erfinder:
- **Rothenburg, Jens**
  72622 Nürtingen (DE)
- **Keller, Fabian**
  72631 Aichtal (DE)

(74) Vertreter: **Ruckh, Rainer Gerhard**
Patentanwalt
Jurastrasse 1
73087 Bad Boll (DE)

(54) ZUGANGSSYSTEM ZU EINER MASCHINE

(57) Die Erfindung betrifft ein Zugangssystem (1) für eine von einer Steuereinheit (6) gesteuerten Maschine (7), mit einer Kontrolleinheit (2) und diesen zugeordneten elektronischen Schlüsseln (3). Die Kontrolleinheit (2) weist eine Leseeinheit (5) auf, mittels derer Daten aus den elektronischen Schlüsseln (3) ausgelesen werden. Die Kontrolleinheit (2) ist über eine Datenverbindung (8) mit der Steuereinheit (6) verbunden. Die elektronischen Schlüssel (3) weisen unterschiedliche Datenbereiche auf, die jeweils einem Anwender zugeordnet und mit einem Verschlüsselungscode gesichert sind. Die Verschlüsselungscodes der Kontrolleinheit (2) sind einlesbar und in einem Speicher 9 speicherbar. Mit der Kontrolleinheit (2) werden Daten aus einem Datenbereich eines elektronischen Schlüssels (3) nur dann ausgelesen und an die Steuereinheit (6) übermittelt, wenn der Verschlüsselungscode dieses Datenbereichs mit einem in die elektronischen Schlüssel (3) eingelesenen Verschlüsselungscode übereinstimmt. Weiter sind elektronische Schlüssel (3) mit Datenbereichen, die jeweils mit einem Verschlüsselungscode eines Anwenders eines zweiten Typs verschlüsselt sind, vorhanden. Diese Verschlüsselungscodes sind im Speicher (10) der Steuereinheit (6) abgespeichert. Einer dieser Verschlüsselungscodes kann in die Kontrolleinheit (2) übertragen werden.

Fig. 1



EP 4 231 256 A1

Beschreibung

[0001] Die Erfindung betrifft ein Zugangssystem zu einer Maschine und ein Verfahren zum Betrieb eines Zugangssystems.

[0002] Derartige Zugangssysteme dienen dazu, den Zugang zu einer Maschine und/oder deren Funktionen im Sinne einer Berechtigung zu schützen und zu kontrollieren. Der Begriff Maschine umfasst dabei auch komplexere Anlagen. Von derartigen Maschinen können generell Gefahren, insbesondere für Personen, ausgehen, so dass der Betrieb der Maschine durch sicherheitstechnische Maßnahmen, wie z. B. Überwachungseinrichtungen, abgesichert werden muss.

[0003] Ein Zugang zu derartigen Maschinen muss dafür gewährt werden, dass an der Maschine bestimmte Funktionen oder Betriebsarten eingestellt werden.

[0004] Bei der Gewährung eines Zugangs zur Maschine müssen insbesondere auch sicherheitstechnische Aspekte berücksichtigt werden. Dies ist beispielsweise dann der Fall, wenn zur Gewährung eines Zugangs einer Person zur Maschine sicherheitstechnische Einrichtungen, wie z. B. Überwachungseinrichtungen überbrückt, d. h. zeitweise außer Kraft gesetzt werden. Dann kann es zu Gefährdungen von Personen kommen, denen Zugang zur Maschine oder deren Vorfeld gewährt wird. In derartigen Fällen darf nur qualifiziertem Sicherheitspersonal Zugang zur Maschine gewährt werden.

[0005] Weiterhin besteht eine Anforderung an derartige Zugangssysteme darin, dass unterschiedlichen Personenkreisen, d. h. Anwendern, Zugang zur Maschine zu gewähren ist.

[0006] Ein erster Typ von Anwender ist der Endanwender der Maschine, d. h. derjenige, der die Maschine zur Durchführung von Arbeitsvorgängen nutzt. Der Endanwender möchte z. B. den Zugang zur Maschine auf einzelne Mitarbeiter beschränken. Dabei soll jeder Mitarbeiter entsprechend seiner Fähigkeiten bzw. Befugnisse einen Zugang zur Maschine in vorgegebenem Umfang bekommen. Der Zugang kann dann auf bestimmte Aktionen, wie z. B. dem Einrichten, Programmieren oder Parametrieren, begrenzt werden.

[0007] Ein zweiter Typ von Anwender ist der Maschinenbauer, der die Maschine herstellt oder in einer Installationsumgebung integriert. Insbesondere bei der Integration der Maschine in einer Installationsumgebung arbeitet die Maschine ohne vollständige Sicherheitseinrichtungen, so dass Gefahren von der Maschine ausgehen können. Daher besteht eine wesentliche Anforderung darin, für derartige Tätigkeiten nur sicherheitstechnisch geschultes Personal des Maschinenbauers Zugang zur Maschine zu gewähren, nicht jedoch dem Personal des Endanwenders.

[0008] Bekannte Zugangssysteme arbeiten passwortgeschützt, d. h. das Zugangssystem gewährt einem Anwender über ein Passwort Zugang zur Maschine. Ein Problem besteht darin, dass Passwörter oft nicht geheim gehalten werden und damit auch Unbefugte Zugang zur Maschine erhalten können.

[0009] Weiterhin sind Zugangssysteme mit Schlüsselwahlschaltern bekannt. Derartige Zugangssysteme bieten nur einen geringen Schutz, da diese Schlüsselwahlschalter aus Unachtsamkeit oft in der entsprechenden Aufnahme stecken gelassen werden, so dass Unbefugte leicht Zugang zur Maschine erlangen.

[0010] Schließlich sind transponderbasierte Zugangssysteme bekannt. Typischerweise werden derartige Zugangssysteme für Endanwender einer Maschine bereitgestellt.

[0011] Ein Nachteil derartiger transponderbasierter Zugangssysteme besteht darin, dass diese nur für einen Typ von Anwender, insbesondere den Endanwender konzipiert sind. Soll das Zugangssystem auch für weitere Typen von Anwendern, wie z. B. den Maschinenbauer, nutzbar gemacht werden, muss der Endanwender vom Maschinenbauer Informationen über die jeweiligen Zugangsmöglichkeiten erhalten, die dann auf dem Transponder zu implementieren sind. Damit aber sind dem Endanwender die vom Maschinenhersteller vorgegebenen Zugangsmöglichkeiten bekannt, was aus Geheimhaltungsgründen unerwünscht ist.

[0012] Daher ist es bekannt, für die unterschiedlichen Typen von Anwendern unterschiedliche Zugangssysteme einzusetzen. Dies stellt jedoch einen unerwünscht hohen Konstruktions- und Kostenaufwand dar.

[0013] Der Erfindung liegt die Aufgabe zugrunde, ein Zugangssystem mit hohem Sicherheitsniveau bereitzustellen.

[0014] Zur Lösung dieser Aufgabe sind die Merkmale der unabhängigen Ansprüche vorgesehen. Vorteilhafte Ausführungsformen und zweckmäßige Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen beschrieben.

[0015] Die Erfindung betrifft ein Zugangssystem für eine von einer Steuereinheit gesteuerten Maschine, mit einer Kontrolleinheit und diesen zugeordneten elektronischen Schlüsseln. Die Kontrolleinheit weist eine Leseeinheit auf, mittels derer Daten aus den elektronischen Schlüsseln ausgelesen werden. Die Kontrolleinheit ist über eine Datenverbindung mit der Steuereinheit verbunden. Die elektronischen Schlüssel weisen unterschiedliche Datenbereiche auf, die jeweils einem Anwender zugeordnet und mit einem Verschlüsselungscode gesichert sind. Die Verschlüsselungscodes sind in die Kontrolleinheit einlesbar und in einem Speicher speicherbar. Mit der Kontrolleinheit werden Daten aus einem Datenbereich eines elektronischen Schlüssels nur dann ausgelesen und an die Steuereinheit übermittelt, wenn der Verschlüsselungscode dieses Datenbereichs mit einem in die elektronischen Schlüssel eingelesenen Verschlüsselungscode übereinstimmt.

[0016] Weiter sind elektronische Schlüssel mit Datenbereichen, die jeweils mit einem Verschlüsselungscode eines Anwenders eines zweiten Typs verschlüsselt sind, vorhanden. Diese Verschlüsselungscodes sind im Speicher der Steuereinheit abgespeichert. Einer dieser Ver-

schlüsselungscodes kann in die Kontrolleinheit übertragen werden.

[0017] Die Erfindung betrifft weiterhin ein entsprechendes Verfahren.

[0018] Der Grundgedanke der Erfindung besteht somit darin, elektronische Schlüssel, die insbesondere von Transpondern gebildet sind, mit unterschiedlichen Datenbereichen, die individuell, d. h. mit verschiedenen Verschlüsselungscodes verschlüsselt und gesichert sind, auszustatten. Wesentlich dabei ist, dass ein Verschlüsselungscode, mit dem ein Datenbereich eines elektronischen Schlüssels verschlüsselt ist, nur dem jeweiligen Anwender bekannt ist, dem dieser elektronische Schlüssel zugeordnet ist, nicht jedoch den anderen Anwendern.

[0019] Elektronische Schlüssel mit unterschiedlichen Datenbereichen sind unterschiedlichen Anwendern, insbesondere auch unterschiedlichen Typen von Anwendern, zugeordnet. Durch die individuelle Verschlüsselung der einzelnen Datenbereiche der einzelnen elektronischen Schlüssel hat jeder Anwender nur Zugang zu dem Datenbereich, der mit dem ihm zugeordneten Verschlüsselungscode verschlüsselt ist, nicht jedoch zu allen anderen Datenbereichen von elektronischen Schlüsseln.

[0020] Damit besteht ein sicherer und vollständiger Schutz gegen ein unbefugtes Lesen von Daten eines Anwenders durch einen weiteren Anwender.

[0021] Ein weiterer wesentlicher Vorteil besteht darin, dass unterschiedliche elektronische Schlüssel mit ihren mit individuellen Verschlüsselungscodes gesicherten Datenbereichen auch unterschiedlichen Typen von Anwendern, insbesondere Endanwender der jeweiligen Maschine oder dem Maschinenbauer, der die Maschine installiert, zugeordnet sein können. Durch die Verschlüsselung der Datenbereiche mit individuellen Verschlüsselungscodes für die einzelnen Datenbereiche ist eine Geheimhaltung derart gewährleistet, dass kein unkontrollierter Datenaustausch zwischen elektronischen Schlüsseln der verschiedenen Typen von Anwendern erfolgt. Damit kann ein Zugangssystem mit nur einer Kontrolleinheit als Zugangskontrolle für unterschiedliche Anwender, insbesondere Endanwender und Maschinenbauer, genutzt werden.

[0022] Die Funktionsweise des erfindungsgemäßen Zugangssystems ist derart, dass als Voraussetzung für einen Zugang zur Maschine zunächst ein oder mehrere Verschlüsselungscodes in die Kontrolleinheit eingelesen und abgespeichert werden.

[0023] Bei Lesen eines elektronischen Schlüssels durch die Kontrolleinheit findet in dieser eine Kontrolle derart statt, dass ein mit einem Verschlüsselungscode verschlüsselter Datenbereich des elektronischen Schlüssels nur dann von der Kontrolleinheit gelesen und an die Steuereinheit übermittelt werden kann, wenn dieser Verschlüsselungscode mit dem oder einem in der Kontrolleinheit abgespeicherten oder an die Kontrolleinheit übergebenen Verschlüsselungscode übereinstimmt.

[0024] Mit den an die Steuereinheit übermittelten Daten erfolgt ein Zugang zur Maschine. Die Daten sind dementsprechend Zugangsdaten, wobei für unterschiedliche Anwender unterschiedliche Zugangsdaten, insbesondere unterschiedliche Zugriffsberechtigungen für die Maschine vorgegeben werden.

[0025] Die Übertragung der Daten von der Kontrolleinheit zur Steuereinheit erfolgt mit einer Datenverbindung, die insbesondere in Form eines Bussystems ausgebildet sein kann. Beispiele für derartige Bussysteme sind Profinet oder Ethernet/IP. Eine weitere Ausführungsform ist eine serielle Schnittstelle, wie z.B. USB.

[0026] Gemäß einer vorteilhaften Ausführungsform der Erfindung ist in jedem elektronischen Schlüssel ein geheimer Datenbereich vorhanden, der mit einem geheimen, nur in der Kontrolleinheit bekannten Verschlüsselungscode gesichert ist.

[0027] In dem geheimen Datenbereich sind Verschlüsselungscodes für Anwender eines ersten Typs gespeichert.

[0028] Da der geheime Verschlüsselungscode nur in der Kontrolleinheit bekannt ist, kann der geheime Datenbereich nur von der Kontrolleinheit ausgelesen werden und ist insbesondere gegen Zugriff aller Anwender geschützt.

[0029] Damit sind die Verschlüsselungscodes für Anwender des ersten Typs gegen unbefugte Zugriffe vollständig geschützt.

[0030] Vorteilhaft handelt es sich bei dem ersten Typ von Anwender um den Endanwender der Maschine.

[0031] Die Vergabe einer Zugangsberechtigung zur Maschine für genau einen Anwender des ersten Typs erfolgt vorteilhaft derart, dass sobald ein Schlüssel dieses Typs gelesen wird, in einem einmalig ablaufenden Initialisierungsprozess die Verschlüsselungscodes genau dieses Anwenders in der Kontrolleinheit abgespeichert werden. Von der Kontrolleinheit werden dazu die Verschlüsselungscodes aus dem geheimen Datenbereich ausgelesen. Elektronische Schlüssel diesen Typs und genau von diesem einen Anwender werden dadurch für eine Datenübertragung mit der Steuereinheit freigegeben.

[0032] Damit werden im Initialisierungsprozess gelesene elektronische Schlüssel des ersten Typs und genau eines Anwenders von der Kontrolleinheit für den Zugang zur Maschine freigegeben. Die Daten dieser elektronischen Schlüssel können von der Kontrolleinheit aus dem Datenbereich ausgelesen und an die Steuereinheit übermittelt werden. Je nach Ausbildung der im elektronischen Schlüssel gespeicherten Zugangsdaten wird dann ein spezifischer Zugang zur Maschine gewährt.

[0033] Prinzipiell können in Initialisierungsprozessen mehrere elektronische Schlüssel in der Kontrolleinheit eingelernt werden, so dass mit diesen elektronischen Schlüsseln ein Zugang zur Maschine ermöglicht wird.

[0034] Vorteilhaft werden mit der Freigabe des im Initialisierungsprozess gelesenen elektronischen Schlüssels genau dieses Anwenders des ersten Typs in der

Kontrolleinheit die anderen elektronischen Schlüssel von anderen Anwendern des ersten Typs mit Datenbereichen, die mit einem anderen Verschlüsselungscode verschlüsselt sind, für eine Datenübertragung mit der Steuereinheit gesperrt.

[0035] In diesem Fall werden singulär nur elektronische Schlüssel genau eines Anwenders des ersten Typs für den Zugang zur Maschine freigegeben.

[0036] Vorteilhaft ist es, wenn die beschriebene Initialisierung nur einmalig bei dem ersten Erkennen eines gültigen elektronischen Schlüssels mit einem Datenbereich des ersten Typs durchgeführt wird.

[0037] Dabei ist es weiter vorteilhaft, dass ein elektronischer Schlüssel mit einem Datenbereich, der mit einem Verschlüsselungscode eines Anwenders des ersten Typs verschlüsselt ist, nur von diesem einen Anwender hergestellt werden kann.

[0038] Damit ist eine unverwechselbare Erstellung von elektronischen Schlüsseln gewährleistet.

[0039] Erfindungsgemäß sind elektronischen Schlüssel mit Datenbereichen, die jeweils mit einem Verschlüsselungscode eines Anwenders eines zweiten Typs verschlüsselt sind, vorgesehen. Diese Verschlüsselungscodes sind nicht in der Kontrolleinheit, aber in der Steuereinheit abgespeichert. Zum Lesen von Schlüsseln des zweiten Typs muss ein Verschlüsselungscode von der Steuereinheit an die Kontrolleinheit übertragen werden.

[0040] Dabei sind die Verschlüsselungscodes in einem geheimen Speicherbereich der Steuereinheit gespeichert.

[0041] Damit sind die Verschlüsselungscodes gegen unbefugte Zugriffe geschützt.

[0042] Mit der Speicherung der Verschlüsselungscodes für Anwender des zweiten Typs in der Steuereinheit wird eine unabhängige Speicherung dieser Verschlüsselungscodes von den Verschlüsselungscodes für Anwender des ersten Typs erzielt. Während es sich bei Anwendern des ersten Typs um Endanwender handelt, handelt es sich bei Anwendern des zweiten Typs vorteilhaft um Maschinenbauer, d. h. Anwender, die die Maschine installieren und in Betrieb nehmen.

[0043] Durch einen von der Steuereinheit an die Kontrolleinheit übermittelten Verschlüsselungscode wird der entsprechende elektronische Schlüssel eines Anwenders des zweiten Typs für eine Datenübertragung mit der Steuereinheit und damit für einen Zugang zur Maschine freigegeben.

[0044] Gemäß einer vorteilhaften Ausgestaltung werden Daten eines Datenbereichs nur eines elektronischen Schlüssels des ersten Typs zyklisch von der Kontrolleinheit an die Steuereinheit übermittelt. Die Daten werden vom Datenbereich weiterer elektronischer Schlüssel des zweiten Typs azyklisch an die Steuereinheit übertragen.

[0045] Gemäß einer weiteren vorteilhaften Ausführung werden Daten sowohl vom Datenbereich des ersten Typs, als auch zweiten Typs als zyklische Daten übertragen.

[0046] Die zyklische Datenübertragung, die beispielsweise im Takt einer in der Kontrolleinheit integrierten Rechnereinheit, d. h. in einem Prozesstakt, erfolgt, erfolgt in erheblich kürzeren Zeitabständen, als die azyklische Datenübertragung.

[0047] Es hat sich als effizient und ausreichend erwiesen, nur die Zugangsdaten des elektronischen Schlüssels eines Anwenders, insbesondere eines Endanwenders, zyklisch zu übertragen, während es für Zugangsdaten eines elektronischen Schlüssels eines zweiten Anwenders, insbesondere des Maschinenbauers, ausreichend ist, diese azyklisch zu übertragen.

[0048] Die Flexibilität des Zugangssystems kann dadurch noch gesteigert werden, dass mittels der Steuereinheit eine Umschaltung der zyklischen und azyklischen Übertragung von Daten von elektronischen Schlüsseln erfolgt.

[0049] Eine Schwachstelle ist die Speicherung des Verschlüsselungscodes in der Steuereinheit sowie die Datenübertragung dieses Verschlüsselungscodes über ein ungesichertes Netzwerk.

[0050] Diese Problematik wird gelöst durch ein Verfahren zum Betrieb eines Zugangssystems für eine von einer Steuereinheit gesteuerten Maschine mit einer Kontrolleinheit und diesen zugeordneten elektronischen Schlüsseln. Die Kontrolleinheit weist eine Leseeinheit auf, mittels derer Daten aus den elektronischen Schlüsseln ausgelesen werden und wobei die Kontrolleinheit über eine Datenverbindung mit der Steuereinheit verbunden ist. Ein Datenbereich eines elektronischen Schlüssels kann mit einem Verschlüsselungscode D entschlüsselt werden, wobei der Verschlüsselungscode D aus zwei Verschlüsselungscodes E, F generiert wird. Der Verschlüsselungscode D wird von der Steuereinheit an die Kontrolleinheit übertragen. Der Verschlüsselungscode F ist auf einem elektronischen Datenträger gespeichert.

[0051] Gemäß einer besonders vorteilhaften Ausgestaltung der Erfindung kann ein Datenbereich eines elektronischen Schlüssels eines Anwenders eines zweiten Typs mit einem Verschlüsselungscode entschlüsselt werden. Der Verschlüsselungscode wird aus zwei Verschlüsselungscodes generiert. Der Verschlüsselungscode wird von der Steuereinheit an die Kontrolleinheit übertragen und im elektronischen Schlüssel gespeichert.

[0052] Mit diesem Verfahren wird auf einfache Weise eine wirksame Absicherung gegen Bekanntwerden des Verschlüsselungscodes zum Erstellen neuer Schlüssel und damit gegen Manipulationen erzielt.

[0053] In Steuerungen können Daten zumeist sehr einfach direkt ausgelesen werden.

[0054] Die Übertragung von Daten von der Steuereinheit zur Kontrolleinheit kann insbesondere über ungesicherte Netzwerke wie z.B. Profinet oder Ethernet/IP erfolgen. Durch Abhörgeräte wie sogenannte Datensniffer können über derartige Netzwerke übertragene Daten, insbesondere auch Verschlüsselungscodes abgehört werden. Wird mit einem so abgehörten Verschlüsselungscode ein Datenbereich eines elektronischen

Schlüssels gesichert, so wird mit dem abgehörten Verschlüsselungscode ein unbefugter Zugang zu dem Datenbereich des elektronischen Schlüssels ermöglicht.

[0055] Diese Schwachstellen werden mit dem erfindungsgemäßen Verfahren eliminiert.

[0056] Der Grundgedanke des erfindungsgemäßen Verfahrens besteht darin, dass der von der Steuereinheit zur Kontrolleinheit übertragene Verschlüsselungscode E zur Entschlüsselung eines Datenbereichs eines elektronischen Schlüssels allein nicht ausreicht. Vielmehr wird der von der Steuereinheit zur Kontrolleinheit übertragene Verschlüsselungscode E mit einem im elektronischen Schlüssel vorhandenen Verschlüsselungscode F zu einem Verschlüsselungscode D kombiniert. Nur mit dem so generierten Verschlüsselungscode D kann der jeweilige Datenbereich des elektronischen Schlüssels entschlüsselt, d.h. ausgelesen und ausgewertet werden.

[0057] Damit ist der Datenbereich des elektronischen Schlüssels gegen unbefugten Zugriff gesichert. Selbst wenn der über ein ggf. ungesichertes Netzwerk übertragene Verschlüsselungscode E von einem Datensniffer oder dergleichen abgehört wird, oder der Verschlüsselungscode aus der Steuerung ausgelesen wird, wird damit kein Zugang zu dem Datenbereich des elektronischen Schlüssels ermöglicht. Ein Zugriff zu dem Datenbereich des elektronischen Schlüssels kann nur mit dem Verschlüsselungscode D erfolgen, der aus dem übertragenen Verschlüsselungscode E und dem im elektronischen Schlüssel vorhandenen Verschlüsselungscode F kombiniert wird. Zur Erhöhung der Manipulationssicherheit kann der Verschlüsselungscode F in einem geschützten Bereich des elektronischen Schlüssels abgelegt sein.

[0058] Gemäß einer ersten Ausführungsform wird der Verschlüsselungscode D aus den Verschlüsselungscodes E, F zur Nutzung eines symmetrischen Verschlüsselungsverfahrens generiert.

[0059] Beispielsweise wird der Verschlüsselungscode D aus den Verschlüsselungscodes E, F mittels einer logischen Beziehung generiert.

[0060] Die logische Beziehung kann eine UND-, eine ODER- bzw. eine XOR-Verknüpfung oder dergleichen oder auch eine beliebige andere Rechenoperation sein.

[0061] Gemäß einer zweiten Ausführungsform wird der Verschlüsselungscode D aus den Verschlüsselungscodes E, F zur Nutzung mit einem asymmetrischen Kryptoverfahren generiert.

[0062] Die Erfindung wird im Folgenden anhand der Zeichnungen erläutert. Es zeigen.

Figur 1: Ausführungsbeispiel des erfindungsgemäßen Zugangssystems.

Figur 2: Generelle Darstellung der Datenstruktur eines elektronischen Schlüssels für das Zugangssystem gemäß Figur 1.

Figur 3: Darstellung eines von einem Endanwender A1 produzierten elektronischen Schlüssels.

Figur 4: Darstellung eines von einem Maschinenbauer B1 produzierten elektronischen Schlüssels.

Figur 5: Zustandsdarstellung des Zugangssystems bevor dessen Kontrolleinheit einen elektronischen Schlüssel gelesen hat ohne Initialisierung.

Figur 6: Zustandsdarstellung des Zugangssystems nach Einführen eines elektronischen Schlüssels des Endanwenders A1 in einem Lesebereich der Kontrolleinheit ohne Initialisierung.

Figur 7: Zustandsdarstellung des Zugangssystems nach Speichern des Verschlüsselungscodes des Endanwenders in der Kontrolleinheit nach Initialisierung.

Figur 8: Zustandsdarstellung des Zugangssystems bei Lesen eines Verschlüsselungscodes eines Schlüssels eines Maschinenbauers.

Figur 9: Weiteres Ausführungsbeispiel des erfindungsgemäßen Zugangssystems.

[0063] Figur 1 zeigt schematisch ein Ausführungsbeispiel des erfindungsgemäßen Zugangssystems 1. Das Zugangssystem 1 weist nur eine Kontrolleinheit 2, der mehrere elektronische Schlüssel 3 zugeordnet sind, auf. Die elektronischen Schlüssel 3 sind im vorliegenden Fall in Form von Transpondern ausgebildet.

[0064] Die Kontrolleinheit 2 weist eine Rechnereinheit 4 auf, die je nach den sicherheitstechnischen Anforderungen an das Zugangssystem 1 aus einer ein- oder mehrkanaligen Prozessorstruktur besteht. Weiterhin weist die Kontrolleinheit 2 eine Leseeinheit 5 in Form eines RFID-Lesegeräts auf. Mit der Leseeinheit 5 können Daten aus einem elektronischen Schlüssel 3 ausgelesen werden, wenn sich dieser innerhalb des Lesebereichs der Leseeinheit 5 befindet. Figur 1 zeigt einen elektronischen Schlüssel 3 innerhalb des Lesebereichs der Leseeinheit 5 und zwei elektronische Schlüssel 3 außerhalb des Lesebereichs. Natürlich kann das Zugangssystem 1 auch eine andere Anzahl von elektronischen Schlüsseln 3 aufweisen. Im Speicher 9 der Kontrolleinheit kann ein Verschlüsselungscode von einem Anwender des ersten Typs gespeichert werden.

[0065] Mit dem Zugangssystem 1 erfolgt ein kontrollierter Zugang zu einer von einer Steuereinheit 6 gesteuerten Maschine 7. Der Begriff Maschine 7 umfasst auch komplexe Anlagen. Die Steuereinheit 6 weist einen Speicher 10 auf. Die Kontrolleinheit 2 kann mit der Steuereinheit 6 bidirektional Daten über eine Datenverbindung 8 austauschen. Die Datenverbindung 8 besteht im vor-

liegenden Fall aus einem Bussystem, wie z. B. Profinet oder Ethernet/IP oder einer seriellen Verbindung, wie z.B. USB.

[0066] Die Funktionsweise des Zugangssystems 1 ist generell derart, dass Zugangsdaten aus den elektronischen Schlüsseln 3 in die Kontrolleinheit 2 eingelesen werden können und die Kontrolleinheit 2 dann die Zugangsdaten an die Steuereinheit 6 übermittelt, wodurch ein kontrollierter Zugang zur Maschine 7 gewährleistet wird.

[0067] Figur 2 zeigt die erfindungsgemäße Struktur des gesamten Datenbereichs eines elektronischen Schlüssels 3, der für alle elektronischen Schlüssel 3 des Zugangssystem 1 identisch aufbaut ist.

[0068] Der elektronische Schlüssel 3 weist einen geheimen Datenbereich C auf, der mit einem Verschlüsselungscode C verschlüsselt ist, der nur in der Kontrolleinheit 2 hinterlegt ist, d. h. der Verschlüsselungscode C ist nur der Kontrolleinheit 2 bekannt.

[0069] Weiterhin sind auf dem elektronischen Schlüssel 3 Datenbereiche A1, A2, ... für Anwender eines ersten Typs, im vorliegenden Fall Endanwender, vorgesehen, wobei A1 dem Endanwender A1 zugeordnet ist, A2 dem Endanwender A2 usw. Die einzelnen Datenbereiche A1, A2, ... sind mit Verschlüsselungscodes A1, A2, ... verschlüsselt.

[0070] Schließlich sind auf dem elektronischen Schlüssel 3 Datenbereiche B1, B2 für Anwender eines zweiten Typs, im vorliegenden Fall eines Maschinenbauers, vorgesehen, wobei B1 dem Maschinenbauer B1 zugeordnet ist, B2 dem Maschinenbauer B2 usw. Die einzelnen Datenbereiche B1, B2, ... sind mit Verschlüsselungscodes B1, B2, ... verschlüsselt.

[0071] Figur 2 zeigt die volle Ausbaustufe von Datenbereichen eines elektronischen Schlüssels 3.

[0072] Figur 3 zeigt einen spezifisch von einem Endanwender A1 produzierten elektronischen Schlüssel 3. Dieser elektronische Schlüssel 3 weist den geheimen Datenbereich C auf, der bei jedem elektronischen Schlüssel 3 in identischer Weise vorhanden ist.

[0073] Darüber hinaus weist der elektronische Schlüssel 3 des Endanwenders A1 nur einen Datenbereich A1, der mit dem Verschlüsselungscode A1 verschlüsselt ist, zu. Der Verschlüsselungscode A1 ist nur dem Endanwender A1 bekannt. Der Datenbereich A1 enthält spezifische, für den Endanwender A1 spezifizierte Zugangsdaten, wie spezielle Zugangsberechtigungen zur Maschine 7.

[0074] Figur 4 zeigt einen spezifisch von einem Maschinenbauer B1 produzierten elektronischen Schlüssel 3. Dieser elektronische Schlüssel 3 weist wieder den geheimen Datenbereich C auf.

[0075] Darüber hinaus weist der elektronische Schlüssel 3 des Maschinenbauers B1 nur einen Datenbereich B1, der mit dem Verschlüsselungscode B1 verschlüsselt ist, zu. Der Verschlüsselungscode B1 ist nur dem Maschinenbauer B1 bekannt. Der Datenbereich B1 enthält spezifische, für den Maschinenbauer B1 spezifizierte Zugangsdaten, wie spezielle Zugangsberechtigungen zur Maschine 7.

[0076] Die Figuren 5 bis 8 veranschaulichen die Funktionsweise des Zugangssystems 1.

[0077] Figur 5 zeigt den Anfangszustand des Zugangssystems 1. In diesem Anfangszustand hat die Kontrolleinheit 2 noch keinen elektronischen Schlüssel 3 gelesen. Demzufolge ist im Speicher der Rechnereinheit 4 der Kontrolleinheit 2 nur der Verschlüsselungscode C für den geheimen Datenbereich C in dem elektronischen Schlüssel 3 hinterlegt.

[0078] In einem geheimen Speicher 10 der Steuereinheit 6 ist der Verschlüsselungscode B1 eines Maschinenbauers hinterlegt.

[0079] Figur 6 zeigt die Situation, wenn der elektronische Schlüssel 3 des Anwenders A1 in den Lesebereich der Leseeinheit 5 der Kontrolleinheit 2 eingebracht wird. Die Kontrolleinheit 2 speichert daraufhin den Verschlüsselungscode A1 in ihrem Speicher 9 ab (dargestellt in Figur 7). Damit kann die Kontrolleinheit 2 den Datenbereich A1 des elektronischen Schlüssels 3 des Anwenders A1 lesen.

[0080] Die von der Kontrolleinheit 2 gelesenen Zugangsdaten des Datenbereichs A1 des elektronischen Schlüssels 3 des Endanwenders A1 werden dann über die Datenverbindung 8 an die Steuereinheit 6 gesendet, wodurch dem Endanwender A1 entsprechend der Zugangsberechtigungen im Datenbereich A1 Zugang zur Maschine 7 gewährt wird.

[0081] Gleichzeitig sperrt die Kontrolleinheit 2 das Lesen aller anderen elektronischen Schlüssel 3 der Endanwender A2, A3, ..., so dass diese nicht mehr gelesen werden können, d. h. die Endanwender A2, A3, ... erhalten keinen Zugang zur Maschine 7. Damit ist die Initialisierung abgeschlossen.

[0082] Jedoch kann der Verschlüsselungscode B1 der im Speicher 10 der Steuereinheit gespeichert ist, von der Steuereinheit 6 an die Kontrolleinheit 2 übertragen und im Speicher der Rechnereinheit 4 temporär hinterlegt werden (Figur 8). Damit kann die Kontrolleinheit 2 den Datenbereich B1 des elektronischen Schlüssels 3 des Maschinenbauers lesen, solange der Schlüssel im Lesebereich bleibt. Die dort enthaltenen Zugangsdaten werden an die Steuereinheit 6 übermittelt, wodurch der Maschinenbauer Zugang zur Maschine 7 erhält. Nach Entfernen des Schlüssels aus dem Lesebereich wird der Verschlüsselungscode B1 in der Rechnereinheit 4 gelöscht.

[0083] Im vorliegenden Fall werden die Zugangsdaten des Datenbereichs A1 des Endanwenders A1 zyklisch übertragen, die Zugangsdaten des Datenbereichs B1 des Maschinenbauers B1 vorzugsweise azyklisch. Durch einen Steuerbefehl kann die Steuereinheit 6 diese Einstellung derart ändern, dass die Zugangsdaten des Datenbereichs B1 zyklisch und die Zugangsdaten des Datenbereichs A1 azyklisch übertragen werden.

[0084] Figur 9 zeigt ein weiteres Ausführungsbeispiel des Zugangssystems mit der Steuereinheit 6, der Kon-

trolleinheit 2 und (exemplarisch) einem elektronischen Schlüssel 3.

[0085] Die Steuereinheit 6 ist mit der Kontrolleinheit 2 über ein Netzwerk 11 verbunden. Das Netzwerk 11 kann ein ungesichertes Netzwerk wie Profinet oder Ethernet/IP sein.

[0086] Weiterhin ist ein Softwaremodul 12 zum Beschreiben von elektronischen Schlüsseln vorhanden, das auf einer geeigneten Rechnerplattform implementiert sein kann.

[0087] Das Softwaremodul 12 beschreibt den elektronischen Schlüssel 3 mit Daten, veranschaulicht durch den Pfeil 13 in Figur 9. Die Daten sind mit einem Verschlüsselungscode D verschlüsselt. Gleichzeitig wird ein Verschlüsselungscode F in einen geschützten Datenbereich des elektronischen Schlüssels 3 geschrieben.

[0088] Das Softwaremodul 12 generiert weiterhin einen Verschlüsselungscode E (Pfeil (14)). Dieser Verschlüsselungscode E wird in der Steuereinheit 6 manuell einprogrammiert (Pfeil (15)).

[0089] Wird im Betrieb des Zugangssystems 1 der elektronische Schlüssel 3 in den Lesebereich der Kontrolleinheit 2 eingebracht, erkennt die Kontrolleinheit 2 den elektronischen Schlüssel 3 und liest den dort gespeicherten Verschlüsselungscode F aus (Pfeil (16)).

[0090] Da der Datenbereich des elektronischen Schlüssels 3 mit dem Verschlüsselungscode D verschlüsselt ist, kann die Steuereinheit 6 diesen Datenbereich noch nicht lesen.

[0091] Die Kontrolleinheit 2 sendet die Information, dass der elektronische Schlüssel 3 in deren Lesebereich ist über das Netzwerk 11 an die Steuereinheit 6. Darauf sendet die Steuereinheit 6 den Verschlüsselungscode E über das Netzwerk 11 an die Kontrolleinheit 2.

[0092] Nun liegen in der Kontrolleinheit 2 der Verschlüsselungscode F des elektronischen Schlüssel 3 und der Verschlüsselungscode E der Steuereinheit 6 vor.

[0093] Die Kontrolleinheit 2 generiert dann aus den Verschlüsselungscodes 4, F den Verschlüsselungscode D wie in Figur 9 schematisch dargestellt.

[0094] Insbesondere wird der Verschlüsselungscode D aus den Verschlüsselungscodes E, F mittels einer logischen Beziehung generiert.

[0095] Alternativ kann der Verschlüsselungscode (D) aus den Verschlüsselungscodes E, F zur Nutzung eines asymmetrischen Kryptoverfahrens generiert werden.

[0096] Nun kann die Kontrolleinheit 2 mittels des generierten Verschlüsselungscodes D den Datenbereich des elektronischen Schlüssel 3 (der mit diesem Verschlüsselungscode D verschlüsselt ist) auslesen.

B ezugszei chenli ste

[0097]

(1) Zugangssystem
(2) Kontrolleinheit
(3) elektronischer Schlüssel
(4) Rechnereinheit
(5) Leseeinheit
(6) Steuereinheit
(7) Maschine
(8) Datenverbindung
(9) Speicher
(10) Speicher
(11) Netzwerk
(12) Softwaremodul
(13) Pfeil
(14) Pfeil
(15) Pfeil
(16) Pfeil

Patentansprüche

1. Zugangssystem (1) für eine von einer Steuereinheit (6) gesteuerten Maschine (7), mit einer Kontrolleinheit (2) und diesen zugeordneten elektronischen Schlüsseln (3), wobei die Kontrolleinheit (2) eine Leseeinheit (5) aufweist, mittels derer Daten aus den elektronischen Schlüsseln (3) ausgelesen werden und wobei die Kontrolleinheit (2) über eine Datenverbindung (8) mit der Steuereinheit (6) verbunden ist, **dadurch gekennzeichnet, dass** die elektronischen Schlüssel (3) unterschiedliche Datenbereiche aufweisen, die jeweils einem Anwender zugeordnet sind und mit einem Verschlüsselungscode gesichert sind, dass in die Kontrolleinheit (2) Verschlüsselungscodes einlesbar und in einem Speicher (9) speicherbar sind, und dass mit der Kontrolleinheit (2) Daten aus einem Datenbereich eines elektronischen Schlüssels (3) nur dann ausgelesen und an die Steuereinheit (6) übermittelt werden, wenn der Verschlüsselungscode dieses Datenbereichs mit einem in die elektronischen Schlüssel (3) eingelesenen Verschlüsselungscode übereinstimmt, und dass elektronische Schlüssel (3) mit Datenbereichen, die jeweils mit einem Verschlüsselungscode eines Anwenders eines zweiten Typs verschlüsselt sind, vorhanden sind, wobei diese Verschlüsselungscodes im Speicher (10) der Steuereinheit (6) abgespeichert sind, und dass einer dieser Verschlüsselungscodes in die Kontrolleinheit (2) übertragen werden kann.

2. Zugangssystem (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** die elektronischen Schlüssel (3) in Form von Transpondern ausgebildet sind.

3. Zugangssystem (1) nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die Daten Zugangsdaten sind.

4. Zugangssystem (1) nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Datenverbindung (8) von einem Bussystem oder einer seriel-

len Schnittstelle gebildet ist.

5. Verfahren zum Betrieb eines Zugangssystems (1) für eine von einer Steuereinheit (6) gesteuerten Maschine (7), mit einer Kontrolleinheit (2) und diesen zugeordneten elektronischen Schlüsseln (3), wobei die Kontrolleinheit(2) eine Leseeinheit (5) aufweist, mittels derer Daten aus den elektronischen Schlüsseln (3) ausgelesen werden und wobei die Kontrolleinheit (2) über eine Datenverbindung (8) mit der Steuereinheit (6) verbunden ist, **dadurch gekennzeichnet, dass** die elektronischen Schlüssel (3) unterschiedliche Datenbereiche aufweisen, die jeweils einem Anwender zugeordnet sind und mit einem Verschlüsselungscode gesichert sind, dass in die Kontrolleinheit (2) Verschlüsselungscodes einlesbar und in einem Speicher (9) speicherbar sind, und dass mit der Kontrolleinheit (2) Daten aus einem Datenbereich eines elektronischen Schlüssels (3) nur dann ausgelesen und an die Steuereinheit (6) übermittelt werden, wenn der Verschlüsselungscode dieses Datenbereichs mit dem im Speicher (9) gespeicherten Verschlüsselungscode übereinstimmt, und dass elektronische Schlüssel (3) mit Datenbereichen, die jeweils mit einem Verschlüsselungscode eines Anwenders eines zweiten Typs verschlüsselt sind, vorhanden sind, wobei diese Verschlüsselungscodes im Speicher (10) der Steuereinheit (6) abgespeichert sind, und dass einer dieser Verschlüsselungscodes in die Kontrolleinheit (2) übertragen werden kann.

6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet, dass** in jedem elektronischen Schlüssel (3) ein geheimer Datenbereich vorhanden ist, der mit einem geheimen, nur in der Kontrolleinheit (2) bekannten, Verschlüsselungscode gesichert ist, wobei in dem geheimen Datenbereich Verschlüsselungscodes für Anwender eines ersten Typs gespeichert sind.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** in einem Initialisierungsprozesses von der Kontrolleinheit (2) ein elektronischer Schlüssel (3) mit einem Datenbereich, der mit einem Verschlüsselungscode eines Anwenders des ersten Typs verschlüsselt ist, gelesen wird, wobei von der Kontrolleinheit (2) die Verschlüsselungscodes aus dem geheimen Datenbereich ausgelesen werden und der mit dem Verschlüsselungscode des gelesenen elektronischen Schlüssels (3) übereinstimmende Verschlüsselungscodes in der Kontrolleinheit (2) im Speicher (9) abgespeichert wird, wodurch elektronische Schlüssel (3) diesen ersten Typs für eine Datenübertragung mit der Steuereinheit (6) freigegeben wird.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet, dass** mit der Speicherung des im Initialisierungsprozess gelesenen Verschlüsselungscodes im Speicher (9) der Kontrolleinheit (2) die anderen elektronischen Schlüssel (3) mit Datenbereichen, die mit einem Verschlüsselungscode von Anwendern des ersten Typs verschlüsselt sind, für eine Datenübertragung mit der Steuereinheit (6) gesperrt werden.

9. Verfahren nach einem der Ansprüche 7 oder 8, **dadurch gekennzeichnet, dass** der Initialisierungsprozess nur einmalig bei dem ersten Erkennen eines gültigen elektronischen Schlüssels (3) mit einem Datenbereich des ersten Typs durchgeführt wird.

10. Verfahren nach einem der Ansprüche 6 bis 9, **dadurch gekennzeichnet, dass** ein elektronischer Schlüssel (3) mit einem Datenbereich, der mit einem Verschlüsselungscode eines Anwenders des ersten Typs verschlüsselt ist, nur von diesem Anwender hergestellt werden kann.

11. Verfahren nach einem der Ansprüche 5 bis 10, **dadurch gekennzeichnet, dass** die Verschlüsselungscodes in einem geheimen Speicherbereich der Steuereinheit (6) gespeichert werden.

12. Verfahren nach einem der Ansprüche 5 bis 11, **dadurch gekennzeichnet, dass** ein Anwender des ersten Typs ein Endanwender ist, und dass ein Anwender des zweiten Typs ein Maschinenbauer ist.

13. Verfahren nach Anspruch 12, **dadurch gekennzeichnet, dass** Daten des Endanwenders zyklisch übertragen werden und Daten des Maschinenbauers azyklisch übertragen werden.

14. Verfahren nach einem der Ansprüche 5 bis 13, **dadurch gekennzeichnet, dass** in der Kontrolleinheit (2) ein elektronischer Schlüssel (3) mit einem Datenbereich, der mit einem Verschlüsselungscode eines Anwenders des zweiten Typs verschlüsselt ist, gelesen werden kann, wenn dieser in der Kontrolleinheit (2) übertragen wird, und dass dann die Übertragung der Daten des Datenbereichs dieses elektronischen Schlüssels (3) an die Steuereinheit (6) freigegeben wird.

15. Verfahren zum Betrieb eines Zugangssystems (1) für eine von einer Steuereinheit (6) gesteuerten Maschine (7), mit einer Kontrolleinheit (2) und diesen zugeordneten elektronischen Schlüsseln (3), wobei die Kontrolleinheit (2) eine Leseeinheit (5) aufweist, mittels derer Daten aus den elektronischen Schlüsseln (3) ausgelesen werden und wobei die Kontrolleinheit (2) über eine Datenverbindung (8) mit der Steuereinheit (6) verbunden ist, **dadurch gekennzeichnet, dass** ein Datenbereich eines elektroni-

schen Schlüssels (3) mit einem Verschlüsselungscode (D) entschlüsselt werden kann, wobei der Verschlüsselungscode (D) aus zwei Verschlüsselungscodes (E, F) generiert wird, wobei der Verschlüsselungscode (E) von der Steuereinheit (6) an die Kontrolleinheit (2) übertragen wird, und wobei der Verschlüsselungscode (F) auf einem elektronischen Datenträger gespeichert ist.

16. Verfahren nach Anspruch 15, **dadurch gekennzeichnet, dass** der Verschlüsselungscode (D) aus den Verschlüsselungscodes (E, F) zur Nutzung eines symmetrischen Verschlüsselungsverfahrens generiert wird.

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** der Verschlüsselungscode (D) aus den Verschlüsselungscodes (E, F) mittels einer logischen Beziehung generiert wird.

18. Verfahren nach Anspruch 15, **dadurch gekennzeichnet, dass** der Verschlüsselungscode (D) aus den Verschlüsselungscodes (E, F) zur Nutzung eines asymmetrischen Kryptoverfahren generiert wird.

19. Verfahren nach einem der Ansprüche 15 bis 18, **dadurch gekennzeichnet, dass** der Datenträger ein elektronischer Schlüssel (3) ist.

Fig. 1

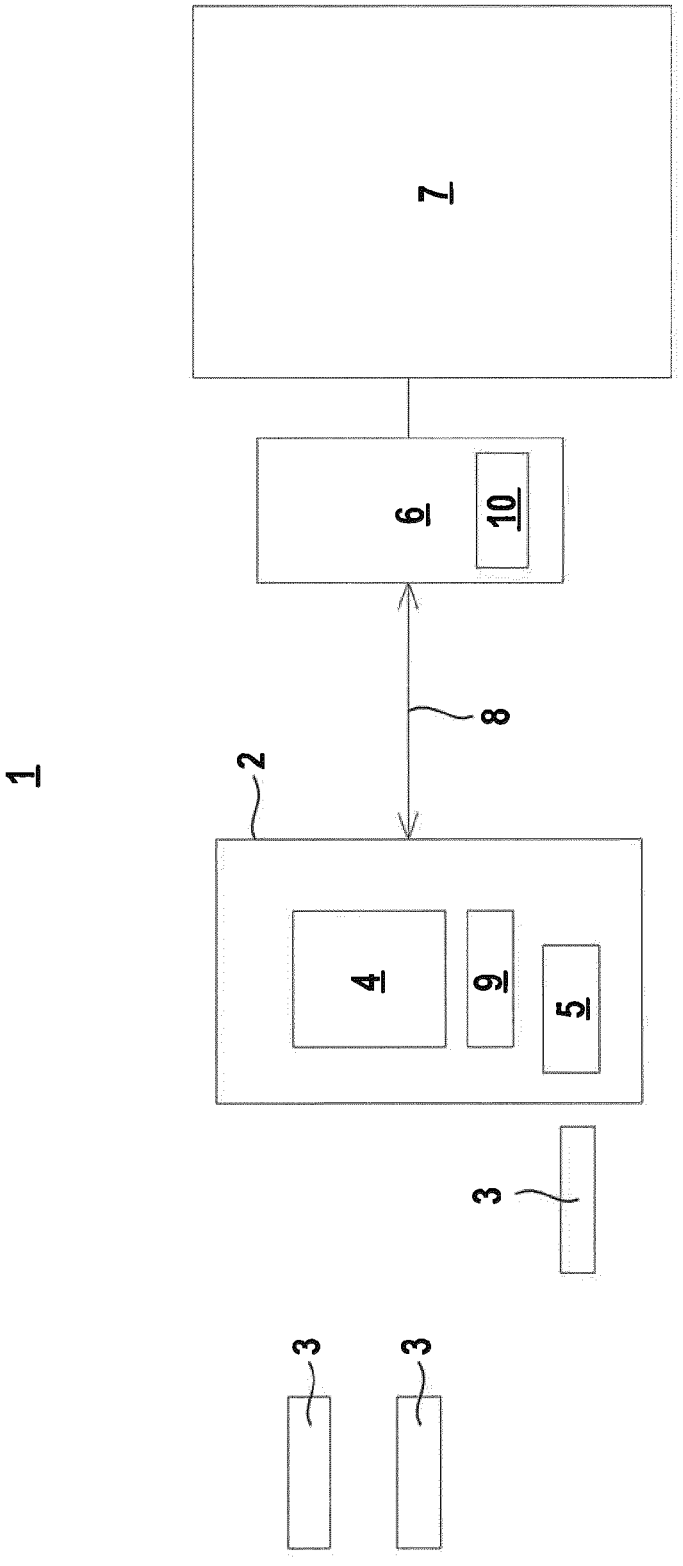


Fig. 2

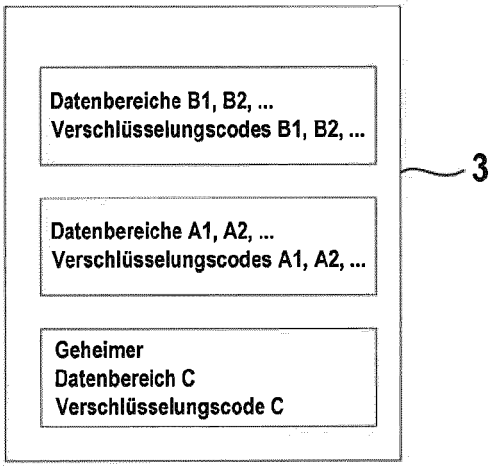


Fig. 3

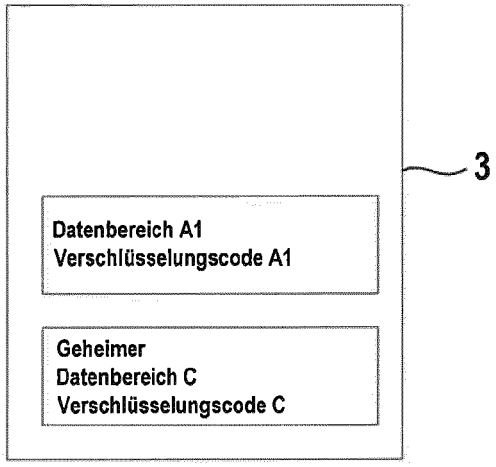
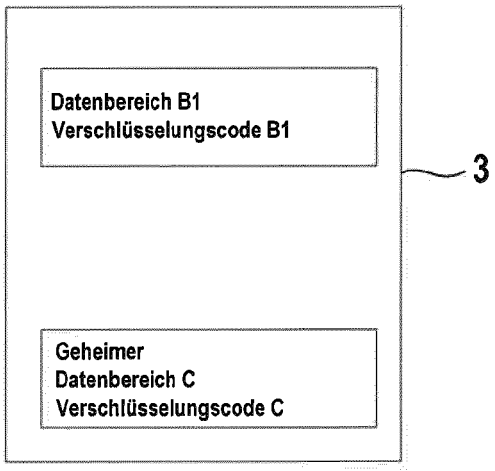
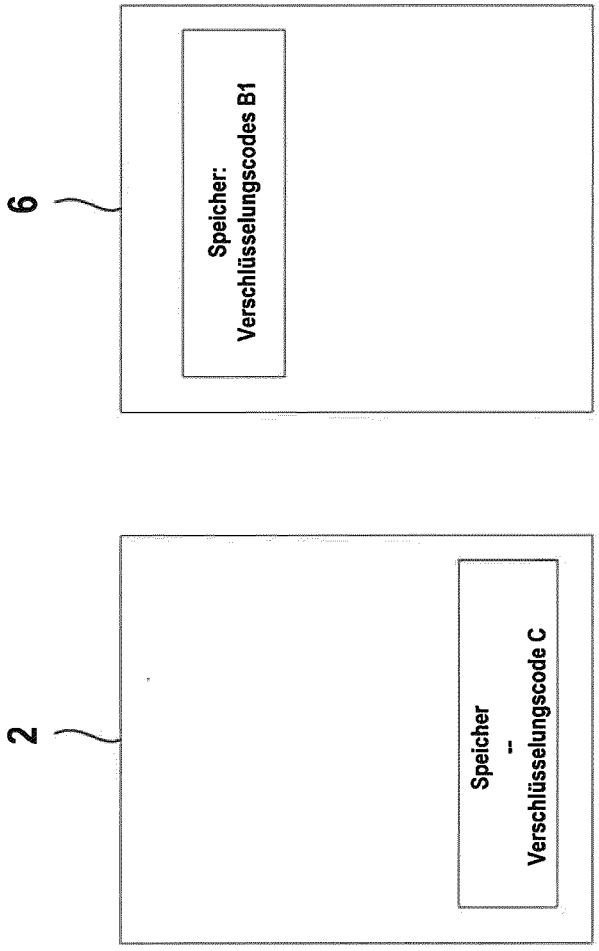


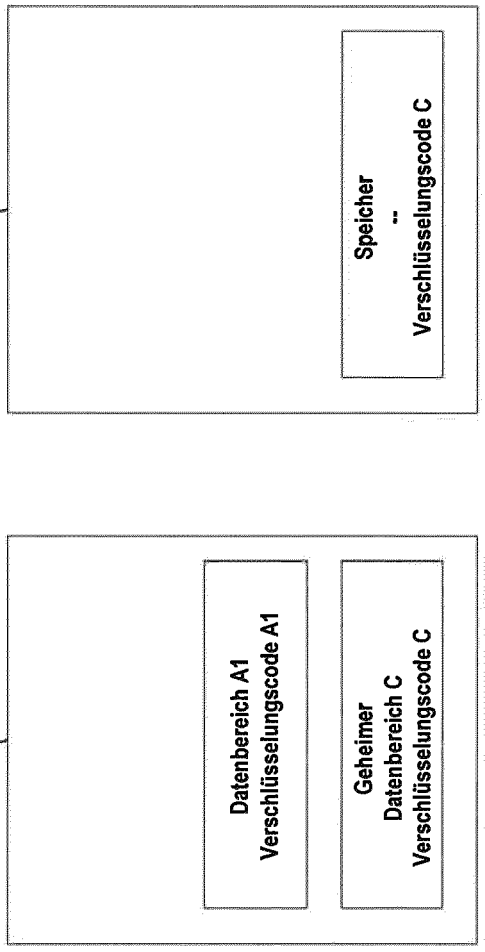
Fig. 4




2
Speicher
--
Verschlüsselungscode C

6
Speicher:
Verschlüsselungscodes B1

Fig. 5


3
Datenbereich A1
Verschlüsselungscode A1
Geheimer
Datenbereich C
Verschlüsselungscode C

2
Speicher
--
Verschlüsselungscode C

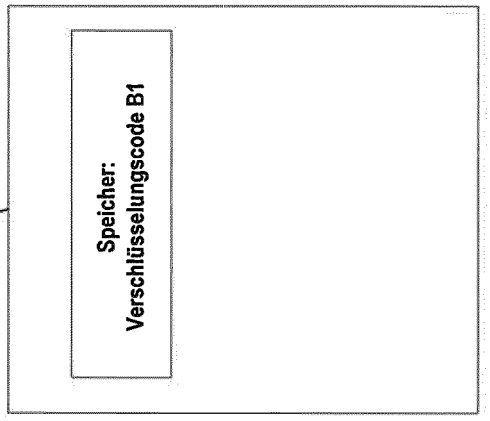

6
Speicher:
Verschlüsselungscode B1

Fig. 6

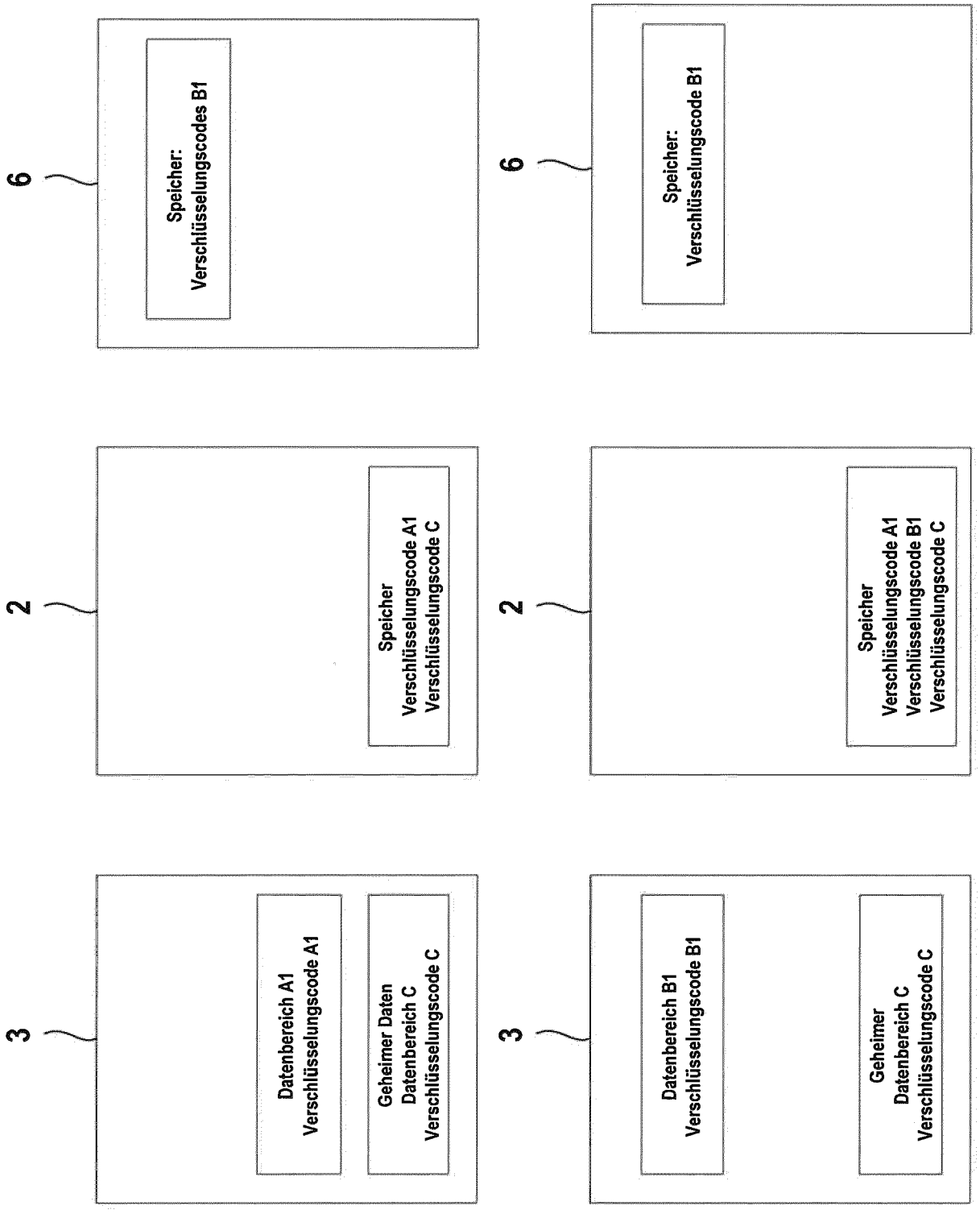

6
Speicher:
Verschlüsselungscodes B1
2
Speicher
Verschlüsselungscode A1
Verschlüsselungscode C
3
Datenbereich A1
Verschlüsselungscode A1
Geheimer Daten
Datenbereich C
Verschlüsselungscode C

Fig. 7

6
Speicher:
Verschlüsselungscode B1
2
Speicher
Verschlüsselungscode A1
Verschlüsselungscode B1
Verschlüsselungscode C
3
Datenbereich B1
Verschlüsselungscode B1
Geheimer
Datenbereich C
Verschlüsselungscode C

Fig. 8

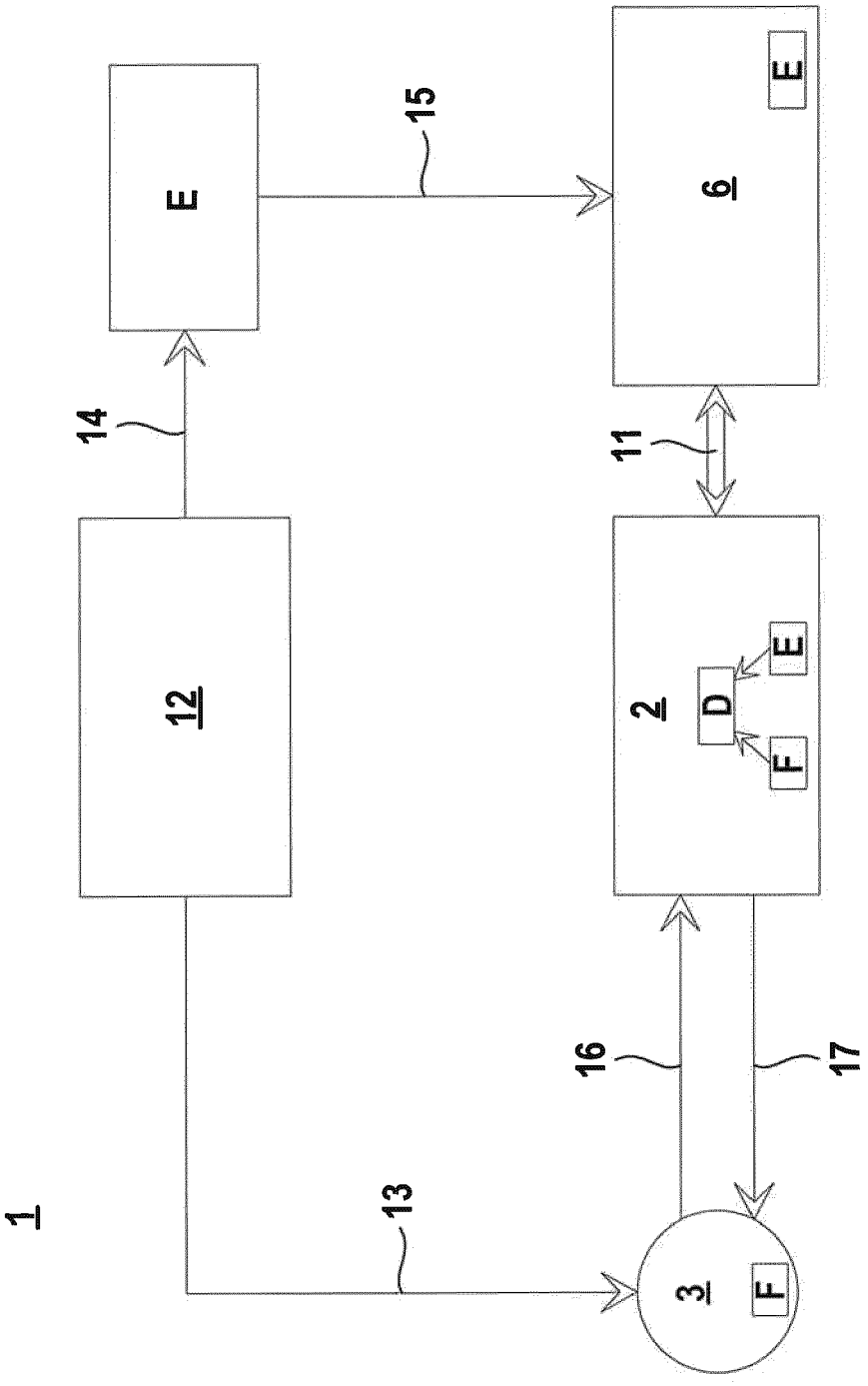


Fig. 9

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 22 20 7943

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
Y	US 6 522 240 B1 (WEISS KARL-ERNST [DE] ET AL) 18. Februar 2003 (2003-02-18) * Zusammenfassung * * Spalte 1, Zeile 64 - Spalte 6, Zeile 4 * * Spalte 6, Zeile 38 - Zeile 57; Abbildungen 1,2 *	1-19	INV. G07C9/00
Y	US 2019/213810 A1 (LUNDBERG FRANS [SE] ET AL) 11. Juli 2019 (2019-07-11) * Absatz [0002] - Absatz [0003] * * Absatz [0008] - Absatz [0009] * * Absatz [0031] - Absatz [0039] * * Absatz [0048] - Absatz [0062] * * Abbildungen *	1-19	
Y	US 2004/201449 A1 (DENISON WILLIAM D [US] ET AL) 14. Oktober 2004 (2004-10-14) * Absatz [0044] - Absatz [0055] * * Abbildungen 5-7 *	7,11	
Y A	US 2014/320261 A1 (DAVIS MICHAEL L [US] ET AL) 30. Oktober 2014 (2014-10-30) * Absatz [0039] - Absatz [0059] * * Absätze [0073], [0091] * * Abbildungen 2,3 *	6 1,5	RECHERCHIERTE SACHGEBIETE (IPC) G07C
Y	US 2018/354460 A1 (BARTELS BASTIAN [DE] ET AL) 13. Dezember 2018 (2018-12-13) * Absatz [0015] - Absatz [0017] * * Absatz [0021] - Absatz [0023] * * Absatz [0028] - Absatz [0032] * * Absatz [0048] - Absatz [0052] *	15-19	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	15. Juni 2023	Miltgen, Eric

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 22 20 7943

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

15-06-2023

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6522240 B1	18-02-2003	AU 734260 B2	07-06-2001
		BR 9805965 A	31-08-1999
		DE 19703998 A1	06-08-1998
		EP 0891607 A1	20-01-1999
		JP 2000509590 A	25-07-2000
		US 6522240 B1	18-02-2003
		WO 9834201 A1	06-08-1998
US 2019213810 A1	11-07-2019	CN 109643474 A	16-04-2019
		EP 3291184 A1	07-03-2018
		KR 20190045201 A	02-05-2019
		US 2019213810 A1	11-07-2019
		US 2021241559 A1	05-08-2021
		WO 2018041905 A1	08-03-2018
US 2004201449 A1	14-10-2004	KEINE	
US 2014320261 A1	30-10-2014	BR 112013023412 A2	27-06-2017
		CN 103609136 A	26-02-2014
		EP 2686839 A2	22-01-2014
		KR 20140019800 A	17-02-2014
		RU 2013146343 A	27-04-2015
		US 2014320261 A1	30-10-2014
		WO 2012125897 A2	20-09-2012
US 2018354460 A1	13-12-2018	CN 109088849 A	25-12-2018
		DE 102017209961 A1	13-12-2018
		EP 3416140 A1	19-12-2018
		US 2018354460 A1	13-12-2018
		US 2021070252 A1	11-03-2021

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82